
**State of Alaska Cyber Security &**
**Critical Infrastructure**
**Cyber Advisory**

**December 8, 2015**

*The following cyber advisory was issued by the State of Alaska and was intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.*

**ADVISORY NUMBER:**
SA2015-142

**DATE(S) ISSUED:**
12/08/2015

**SUBJECT:**
Multiple Vulnerabilities in Microsoft Silverlight Could Allow Remote Code Execution (MS15-129)

**OVERVIEW:**
Multiple vulnerabilities have been discovered in Microsoft Silverlight. The most severe of these vulnerabilities could allow remote code execution. Microsoft Silverlight is a web browser plug-in. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

**THREAT INTELLIGENCE:**
There are currently no reports of these vulnerabilities being exploited in the wild.

**SYSTEMS AFFECTED:**
- Microsoft Silverlight 5
- Microsoft Silverlight 5 Developer Runtime

**RISK:**
**Government:**
- Large and medium government entities: **High**
- Small government entities: **High**

**Businesses:**
- Large and medium business entities: **High**
- Small business entities: **High**

**Home users: High**

**TECHNICAL SUMMARY:**

Three vulnerabilities have been discovered in Microsoft Silverlight, the most severe of which could allow for remote code execution (CVE-2015-6166). This vulnerability occurs when Microsoft Silverlight incorrectly handles certain open and close requests that could result in read and write access violations. To exploit the vulnerability, an attacker could host a website that contains a specially crafted Silverlight application and then convince a user to visit the compromised website. Attackers could also take advantage of websites containing specially crafted content, including those that accept or host user-provided content or advertisements. Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Details of the other vulnerabilities included in this update are as follows:

- Two information disclosure vulnerabilities exist when Silverlight fails to properly handle objects in memory, which could allow an attacker to more reliably predict pointer values and degrade the efficacy of the Address Space Layout Randomization security feature. (CVE-2015-6114 and CVE-2015-6165)

**RECOMMENDATIONS**:

We recommend the following actions be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments, especially those from un-trusted sources.

**REFERENCES:**

**Microsoft:**

https://technet.microsoft.com/en-us/library/security/MS15-129

**CVE:**

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6114
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6165
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6166